This packet includes two versions of a first affirmative constructive (1AC) and extension evidence for the second affirmative constructive (2AC) and the first affirmative rebuttal (1AR). It also includes some negative case arguments.

The 1AC below is called Beyond the Freedom Act and every element is carefully designed to achieve particular argumentative ends, sometimes large and sometimes more subtle. It illustrates several general principles for creating a powerful and effective 1AC you should consider as you imagine ways to make it better and as you design others 1ACs. Like all arguments you encounter, adapt this evidence and these arguments to meet your needs.

**1. The 1AC is important**. The 1AC is not just a collection of evidence making a series of arguments. It should be a story, a coherent narrative that is logically structured and carefully shaped for maximum effect. Debate educators often stress the importance of final rebuttals and the interaction of the negative block (1NC and 1NR) and the 1AR. They are important, obviously. Arguably the 1AC is the most important speech in a debate. For affirmatives, it should be *the* most important speech and, if it is, they will very likely win the debate. ‘Most important’ does not mean ignoring other arguments in favor of those in the 1AC. It means the opposite: anticipating negative arguments and designing the 1AC with foresight to make winning easier.

2) The 1AC **should operate *performatively* and *argumentatively***, and at several levels.

More than any other speech in the debate the 1AC should include specific efforts to create a persuasive speech that is delivered in a way that moves audiences, particularly judges.

Even if it is true that making lots of arguments with evidence in a highly technical fashion constitutes quality debate (and it does not, at least not invariably) the 1AC is typically the speech where such an approach is the least useful, even counterproductive.

When reading speech text, the variation in text size (and underlining and other formatting) draws attention to particular portions of the evidence and parts of arguments. It can also be used to make performing a 1AC more effective, making everything easy to read and understand in the context of *delivering* a 1AC (hard to read compels focus on text which precludes attention to judge). More than other speeches in a debate the affirmative should write a 1AC that is sufficiently memorized, at least in parts, so that direct eye contact and non-verbal communication with the judge is optimized.

Argumentatively a 1AC should establish all the basic requirements of policy or other advocacy: ‘here’s a problem and here is what we think should be done about it’. It should also carefully choose language for argumentative purposes. For instance, if you know the critique your opponent is likely to present, you can include preemptive language in the tags or descriptors of your evidence or argument. Successful framing or repetition of key terms can have an argumentative effect over and above the content of the argument.

3) **Every word plays a role**

Given essentially unlimited prep time, the 1AC affords an opportunity for effective wordsmithing

For instance, I call this Beyond the Freedom Act 1AC for two core purposes. First, it establishes a comparison in which the Freedom Act represents the status quo that the 1AC argues should be ‘moved beyond’. ‘Moved beyond’ is strategically ambiguous: Is the Act good or bad, according the affirmative? The answer is “good enough” to trigger the negative disadvantages and critiques but not good enough to achieve the solvency described in the 1AC. The core comparison is plan compared to the new world of the Freedom Act. Second, by anchoring the debate in a discussion of the Freedom Act, the 1AC preemptively answers some links and uniqueness claims affirmatives are likely to face. Imagine a negative that argues the 1AC causes some undesirable effect. To the degree the 1AC involves or is perceived to involve steps like those taken in the Freedom Act, passed in June 2015, either a) the undesirable effect is inevitable because the recent passage of the Freedom Act will cause it to happen (both the timing and similarity are parts of this argument) or b) if the Freedom Act won’t cause that negative consequence, then the plan in the 1AC will not cause it to happen. The negative effect cannot both link to the plan and do so uniquely.

**4) Simplicity is the origin of nuance**

Many people believe that dense prose featuring complex phrases and clauses and featuring obscure words many syllables long. Those people are wrong as such practices are efforts to create the illusion of profundity where none exists. Keep your language clean and easy to understand. Educated persons do not require opaque text to engage complex and important topics. Keep things simple and then clarify the nuances through your argumentation.

2015 OGDI 1st Affirmative:

Beyond the Freedom Act

The expansive assertions of legal authority used for mass surveillance since 9-11, in particular, the Patriot Act and the FISA Amendments Act of 708, are relatively new and unique in the long history of government surveillance. New legal authorities and new interpretations have conferred previously unimaginable surveillance powers that are in turn massively improved and enabled by new technologies and social practices. Domestic government surveillance programs target every type of electronic communications, including, bulk telephony meta-data under Section 2015 of the Patriot Act and email and all other internet-based digital communications and activities under Sec. 702 of the FAA of 2008 and Executive Order 12333.

Following several years of debate in Congress over a variety of proposals, the Senate passed the USA Freedom Act in early June 2015, over the objections of most Republicans, including McConnell in the Senate and Boehner and Rogers in the House, and a handful of Democrats. In alliance with the White House, Freedom Act opponents were able to significantly water-down final bill ultimately signed by President Obama.

This packet includes a first affirmative constructive (1AC) and extension evidence for the second affirmative constructive (2AC) and the first affirmative rebuttal (1AR). It also includes some negative case arguments. The affirmative advocates adoption of the Surveillance State Repeal Act (1466)

Beyond the Freedom Act:

Surveillance State Repeal Act

Government reports and journalism confirm the reality of pervasive government surveillance unprecedented in its granularity and totality.

Responding to public outrage, in June 2015 Congress passed and President Obama signed the bi-partisan USA Freedom Act, the first “policy win” in decades for reformers, one that most policy elites believe serves the so-called war on terrorism.

Despite perceptions, the Act does not curtail domestic government surveillance but instead entrenches unwarranted intrusions on privacy, trades contrived for real risks, masks the emerging Surveillance State, and undermines internet freedom.

Obs 1: Freedom Act doesn’t curtail domestic surveillance

First, massive warrantless surveillance remains authorized

Freedom of the Press Foundation 2015

[Trevor Timm, Our Statement on Congress passing the USA Freedom Act, the NSA ‘Reform’ Bill, June 2, 2015, https://freedom.press/blog/2015/06/our-statement-congress-passing-usa-freedom-act-nsa-reform-bill

Today the Senate passed a version of the USA Freedom Act, a bill touted by its authors as surveillance reform that will end the NSA’s mass, suspicion-less collection of Americans’ personal data. Given that parts of the Patriot Act expired on June 1st, and that the government is pretending the expiration is a “crisis” rather than an opportunity, President Obama is expected to sign the bill as soon as possible. While the bill has many significant flaws, the USA Freedom Act vote is also historic: it’s the first time since the 1970s that Congress has indicated its intention to restrict the vast powers of intelligence agencies like the NSA, rather than exponentially expand them. It also shows the power that investigative journalism and brave whistleblowing can have on even the most entrenched government interests. Two years ago, debating these modest changes would’ve been unthinkable, and it is absolutely a vindication for Edward Snowden. Unfortunately, the bill is also woefully inadequate and largely symbolic, and Congress would’ve been better off letting Section 215 of the Patriot Act expire permanently. The USA Freedom Act supposedly bans bulk collection of phone records or any other private records, and we certainly hope it actually does. But its provisions are vague and confusing, leading many legal experts to believe they could be re-interpreted in secret—by NSA lawyers with a history of warping the common definitions of ordinary words beyond recognition—and could lead the FISA court to continue to allow the NSA to collect large quantities of Americans’ data in secret. (The administration will shamefully now re-start the phone program that expired on Monday for six months, as allowed under the new law's "transition" period.) The ultra-secret FISA court, a Kafkaesque nightmare for civil liberties, also gets to keep many of its worst features, with just minor changes around the edges. Such an anathema to democracy should be dismantled entirely. The USA Freedom Act also does not touch on two of the NSA’s most powerful and controversial tools: the FISA Amendments Act and Executive Order 12333, which have been used to scan untold billions of emails coming in and out of the United States, and give the agency free rein to spy on 95% of the world’s population with virtually no restrictions.

Second, the Freedom Act masks codification of surveillance

-Bipartisan, inter-branch support due to perception the Act is a key tool in the so-called War on Terror.

Solomon, Exec Dir Inst for Public Accuracy, June 2015

[Normon, Executive Director Institute for Public Accuracy, veteran media critic, “Retooling the Patriot Act”, June 5-7, 2015, Counterpunch, <http://www.counterpunch.org/2015/06/05/retoolingthepatriotact/>

Some foes of mass surveillance have been celebrating the final passage of the USA Freedom Act, but Thomas Drake sounds decidedly glum. The new law, he tells me, is "a new spy program." It restarts some of the worst aspects of the Patriot Act and further codifies systematic violations of Fourth Amendment rights. In Oslo as part of a "Stand Up For Truth" tour, Drake warned at a public forum on Wednesday that "national security" has become "the new state religion." Meanwhile, his Twitter messages were calling the USA Freedom Act an "itty-bitty step" -- and a "stop/restart kabuki shell game" that "starts with restarting bulk collection of phone records." That downbeat appraisal of the USA Freedom Act should give pause to its celebrants. Drake is a former senior executive of the National Security Agency -- and a whistleblower who endured prosecution and faced decades in prison for daring to speak truthfully about NSA activities. He ran afoul of vindictive authorities because he refused to go along with the NSA's massive surveillance program after 9/11. Drake understands how the NSA operates from the highest strategic levels. He notes a telling fact that has gone virtually unacknowledged by anti-surveillance boosters of the USA Freedom Act: "NSA approved." So, of course, did the top purveyor of mendacious claims about the U.S. government's surveillance programs -- President Obama -- who eagerly signed the "USA Freedom" bill into law just hours after the Senate passed it. A comparable guardian of our rights, House Speaker John Boehner, crowed: "This legislation is critical to keeping Americans safe from terrorism and protecting their civil liberties." While some organizations with civil-liberties credentials have responded to the USA Freedom Act by popping open champagne bottles at various decibels, more sober assessments have also been heard. Just after senators approved the bill and sent it to the president, Demand Progress issued a statement pointing out: "The Senate just voted to reinstitute certain lapsed surveillance authorities -- and that means that USA Freedom actually made Americans less free." Another astute assessment came from CREDO, saying that Congress had just created "sweeping new authorities for the government to conduct unconstitutional mass surveillance of Americans." As it happened, the president signed the USA Freedom Act into law while four U.S. "national security" whistleblowers -- Drake as well as Coleen Rowley (FBI), Jesselyn Radack (Justice Department) and Daniel Ellsberg (Pentagon Papers) -- were partway through a "Stand Up For Truth" speaking tour from London to Oslo to Stockholm to Berlin. Traveling as part of the tour, I've been struck by the intensity of interest from audiences in the countries we've already visited -- Great Britain, Norway and Sweden -- where governments have moved to worsen repressive policies for mass surveillance. Right now, many people in Europe and elsewhere who care about civil liberties and want true press freedom are looking at the United States: to understand what an aroused citizenry might be able to accomplish, seeking to roll back a dangerous accumulation of power by an ostensibly democratic government. Let's not unwittingly deceive them -- or ourselves -- about how much ground the U.S. surveillance state has lost so far.

Plan

The United States should curtail its domestic surveillance by passing HR 1466, the State Surveillance Repeal Act, through Congress which President Obama should sign and the US Supreme Court should uphold

Please ask for clarification.

Obs 2: SSRA ends warrantless dragnet surveillance

First, SSRA provides comprehensive protection against mass warrantless surveillance by the State

**-Removes or narrows overly-broad legal authorities**

**-Requires warrants, protects whistleblowers, closes backdoors**

Udry June 2015, Ex Dir Defending Dissent Foundation

(Sue Udry (“Next Step After USA Freedom: Repeal The Surveillance State” http://www.defendingdissent.org/now/author/sue-udry/,June 17, 2015)

On June 1, the U.S. Senate allowed three provisions of the USA PATRIOT Act to expire. A few days later Congress enacted, and the President signed the USA Freedom Act, which introduced modest reforms to NSA mass surveillance. Everyone involved recognized that the bill was only a small reform. What’s next? What can Congress do to roll back unwarranted surveillance? The answer is the Surveillance State Repeal Act introduced by Representatives Mark Pocan (D-WI) and Thomas Massie (R-KY).

True to its name, the bill would repeal the two most notorious post-9/11 dragnet-surveillance laws and overhaul the National Security Agency’s domestic surveillance program. It’s an exceptionally strong and comprehensive bill supported by many civil-liberties organizations, including the Defending Dissent Foundation. In addition to repealing both the USA PATRIOT Act and the FISA Amendments Act, HR 1466 would reinstate a uniform standard requiring warrants based on probable cause for surveillance requests, and prohibit the federal government from forcing technology companies to build hardware or software “back doors” that allow its agencies to bypass encryption or privacy technology. The bill includes some legal protections for national-security whistleblowers, as well as changes to the Foreign Intelligence Surveillance Court to give it greater expertise in reviewing and challenging executive-branch applications for surveillance operations.

Second, the SSRA closes gaps in the Freedom Act

Bill of Rights Committee/Defending Dissent Fndn, 2015

[“USA Freedom And The Surveillance State: The Debate is Only Just Beginning, June 2nd, 2015 https://www.popularresistance.org/usa-freedom-and-the-surveillance-state/]

The Bill of Rights Committee/Defending Dissent Foundation opposes the USA Freedom Act, and calls for a thorough congressional investigation into the surveillance authorities US intelligence agencies have claimed to gather the private information without a warrant of US persons who are not under suspicion of any crime. “Hundreds of thousands of Americans have joined the debate over unwarranted mass surveillance in the last two weeks, and over the last two years since the first Snowden revelation,” said Sue Udry, Executive Director of BORDC/DDF. “Massive trans-partisan civic participation has forced Congress for the first time to take action (albeit woefully inadequate) to rein in some unconstitutional spying.” Along with allies across the political spectrum, BORDC/DDF calls on Congress to use the expiration of Section 215 as a starting point for reforming the out of control surveillance practices of US intelligence agencies. Although the USA Freedom Act includes modest reforms, the FBI, NSA, and other intelligence agencies will be allowed to continue to collect private information about Americans who are under no suspicion of crime under Executive Order 12333 and the FISA Amendments Act. BORDC/DDF calls on Congress to pass the Surveillance State Repeal Act in order to bring surveillance programs in line with the Constitution. “We need a new Church Committee,” Udry said, referring to the Senate Select Committee to Study Governmental Operations that investigated intelligence operations in the 1970s and found significant wrongdoing. “Congress continues to operate in willful ignorance, refusing to demand a full accounting of all surveillance programs our intelligence agencies are using to gather information about innocent Americans. Without Snowden, neither Congress nor the people would have been aware of the NSA’s bulk data collection. What else is going on behind our backs?” Beyond the mass surveillance authorities in the bill, BORDC/DDF is concerned that transparency provisions are inadequate, and specifically exempt the FBI. This is particularly galling given a Department of Justice (DOJ) Inspector General report released two weeks ago that confirms the FBI has been using Section 215 to collect internet records in bulk , and violated the law regarding minimizing records for seven years. Further, the bill includes an increase to the maximum sentence for material support of terrorism, an unacceptably vague and expansive law that does not require a person to engage in or plan to engage in terrorism, or even knowingly support terrorism to be prosecuted. Since 9/11, the statute has become a favorite catch-all for the DOJ into which all sorts of constitutionally protected activities can be thrown and classified as suspect, if not criminal.

Third, whistleblower protections needed for real reform

Benkler 2014, Harvard Law School and Co-Director of

Berkman Center for Internet and Society

[Yochai, “A Public Accountability Defense for National Security Leakers and Whistleblowers“, 8(2) Harv. Rev. L. & Policy, July 2014]

If legitimacy crisis, rather than technological change, is the primary driver of the increase since 2002 of the particular class of leaks that is most important in a democracy, then the present prosecutorial deviation from a long tradition of using informal rather than criminal sanctions19 represents a substantial threat to democracy. In particular, it threatens public accountability for violations of human and civil rights, abuses of emergency powers, and unchecked expansion of the national security establishment itself. Seen in that light, aggressive prosecutions are merely a symptom of the self-same post-9/11 national security overreach that instigated the legitimacy crisis: they manifest the government’s need to shield its controversial actions from public scrutiny and debate.

Criminal liability for leaking and publishing classified materials is usually discussed in terms of a conflict between high-level values: security and democracy. Here, I propose that the high-level abstraction obscures the fact that “national security” is, first and foremost, a system of organizations and institutions, subject to all the imperfections and failures of all other organizations. Considering that the Senate Select Committee on Intelligence (“SSCI”) excoriated the CIA for groupthink failures in the lead up to the invasion of Iraq, and again for its failures and dissembling in conducting its torture interrogation program, it would be naïve beyond credulity to believe that the CIA, NSA, FBI, and Pentagon are immune to the failure dynamics that pervade every other large organization, from state bureaucracies to telecommunications providers, from automobile manufacturers to universities. When organizations that have such vast powers over life and death as well as human and civil rights, the risks of error, incompetence, and malfeasance are immeasurably greater than they are for these other, more workaday organizations. The Maginot Line did not make France more secure from Germany and neither torture nor the invasion of Iraq, with its enormous human, economic, and strategic costs, made America safer from terrorism, weapons of mass destruction, or rogue regimes. A mechanism for identifying and disrupting the organizational dynamics that lead to such strategic errors is necessary for any system of government, and in a democracy that mechanism is the principle of civilian control: fundamental questions of war and peace require public understanding and public decision.

Secrecy insulates self-reinforcing internal organizational dynamics from external correction. In countering this tendency, not all leaks are of the same fabric. “War story”-type leaks that make an administration look good or are aimed to shape public opinion in favor of an already-adopted strategy or to manipulate support for one agency over another, trial balloons, and so forth, are legion.23 While these offer the public color and texture from inside the government and are valuable to the press, they do not offer a productive counterweight to internal systemic failures and errors. Some leaks, however, provide a critical mechanism for piercing the national security system’s echo-chamber, countering self-reinforcing information cascades, groupthink, and cognitive biases that necessarily pervade any closed communications system. It is this type of leak, which exposes and challenges core systemic behaviors, that has increased in this past decade, as it did in the early 1970s. These leaks are primarily driven by conscience, and demand accountability for systemic error, incompetence, or malfeasance. Their critical checking function derives from the fact that conscience is uncorrelated with well-behaved organizational processes. Like an electric fuse, accountability leaks, as we might call them, blow when the internal dynamics of the system reach the breaking point of an individual with knowledge, but without authority. They are therefore hard to predict, and function like surprise inspections that keep a system honest. By doing so, these leaks serve both democracy and security.

This failsafe view of whistleblowing is hardly unique to national security. American law in general embraces whistleblowing as a critical mechanism to address the kinds of destructive organizational dynamics that lead to error, incompetence, and abuse. In healthcare, financial, food and drug, or consumer product industries; in state and federal agencies, throughout the organizational ecosystem, whistleblowers are protected from retaliation and often provided with financial incentives to expose wrongs they have seen and subject the organizations in which they work to public or official scrutiny.25 Whistleblowing is seen as a central pillar to address government corruption and failure throughout the world. Unless one believes that the national security establishment has a magical exemption from the dynamics that lead all other large scale organizations to error, then whistleblowing must be available as a critical arrow in the quiver of any democracy that seeks to contain the tragic consequences that follow when national security organizations make significant errors or engage in illegality or systemic abuse.

# Advantage 1: The Clampdown

The sprawling web of surveillance stifles dissent, disables movements, and unconscionably targets minorities.

First, pervasive surveillance inhibits the exploration, dissemination and sharing of ideas and experiences

Richards 2013, Wash University Law Prof

[Neil, Dangers of Surveillance, 126 Harv. L. Rev. 1934 2012-2013, p. 1948-1950]

Three different kinds of arguments highlight the ways in which surveillance can restrain intellectual activities. The first set of arguments relies on cultural and literary works exploring the idea that surveillance deters eccentric or deviant behavior. Many such works owe a debt to Jeremy Bentham's idea of the Panopticon, a prison designed around a central surveillance tower from which a warden could see into all of the cells. In the Panopticon, prisoners had to conform their activities to those desired by the prison staff because they had no idea when they were being watched. As Bentham describes this system, "[t]o be incessantly under the eyes of an Inspector is to lose in fact the power of doing ill, and almost the very wish.”75 Of course, the most famous cultural exploration of the conforming effects of surveillance is Orwell's harrowing depiction in *Nineteen Eighty-Four* of the totalitarian state personified by Big Brother.76 Orwell's fictional state sought to prohibit not just verbal dissent from the state but even the thinking of such ideas, an act punished as "thought-crime" and deterred by constant state surveillance. 77 Some scholars have documented how the modern surveillance environment differs from both the classic Panoptic on and a fully realized Big Brother in important ways.78 Nevertheless, Orwell's insight about the effects of surveillance on thought and behavior remains valid - the fear of being watched causes people to act and think differently from the way they might otherwise. Our cultural intuitions about the effects of surveillance are supported by a second set of arguments that comes from the empirical work of scholars in the interdisciplinary field of surveillance studies. Moving beyond the classic metaphors of the Panopticon and Big Brother, these scholars have tried to understand modern forms of surveillance by governments, companies, and individuals in all of their complexities. 79 The scope of this burgeoning literature has been wide-ranging and provides many examples of the normalizing effects of surveillance in a wide variety of contexts. In his pioneering work in the 1980s, for example, Professor Anthony Giddens argues that surveillance continually seeks the supervision of social actors and carries with it a permanent risk that supervision could lead to domination.80 More recent scholars have explored the risks that surveillance poses to democratic self-governance.81 One such risk is that of self-censorship, in terms of speech, action, or even belief. Studies of communist states give social-scientific accounts of many of the cultural intuitions about these self-censoring effects of surveillance,82 but so too do studies of modern forms of surveillance in democratic societies. For example, one study of the ED Data Retention Directive notes that "[u]nder pervasive surveillance, individuals are inclined to make choices that conform to mainstream expectations."83 As I explore below, the scope of surveillance studies is much broader than merely the study of panoptic state surveillance; scholars working in this field have examined the full scope of modern forms of watching, including data surveillance by private actors. But above all, surveillance scholars continually reaffirm that, while surveillance by government and others can have many purposes, a recurrent purpose of surveillance is to control behavior.84 A third and final set of arguments for intellectual privacy comes from First Amendment doctrine. A basic principle of free speech law as it has developed over the past century is that free speech is so important that its protection should err on the side of caution. Given the uncertainty of litigation, the Supreme Court has created a series of procedural devices to attempt to ensure that errors in the adjudication of free speech cases tend to allow unlawful speech rather than engage in mistaken censorship. These doctrines form what Professor Lee Bollinger calls the "First Pillar" of First Amendment law - the "[e]xtraordinary [p]rotection against [c]ensorship."85 Such doctrines take various forms, such as those of prior restraint, overbreadth, and vagueness, but they are often characterized under the idea of the "chilling effect." This idea maintains that rules that might deter potentially valuable expression should be treated with a high level of suspicion by courts. As the Supreme Court put it in perhaps its most important free speech decision of the twentieth century, *New York Times Co. v. Sullivan,86* the importance of uninhibited public debate means that, although "erroneous statement is inevitable in free debate, ... it must be protected if the freedoms of expression are to have the 'breathing space' that they 'need ... to survive. "'87

As Professor Frederick Schauer explains, "the chilling effect doctrine recognizes the fact that the legal system is imperfect and mandates the formulation of legal rules that reflect our preference for errors made in favor of free speech."88 Although the chilling-effect doctrine has been criticized on grounds that it overprotects free speech and makes empirically unsupported judgments,89 such criticisms miss the point. The doctrines encapsulated by the chilling effect reflect the substantive value judgment that First Amendment values are too important to require scrupulous proof to vindicate them, and that it is (constitutionally speaking) a better bargain to allow more speech, even if society must endure some of that speech's undesirable consequences. Intellectual-privacy theory explains why we should extend chilling-effect protections to intellectual surveillance, especially traditional-style surveillance by the state. If we care about the development of eccentric individuality and freedom of thought as First Amendment values, then we should be especially wary of surveillance of activities through which those aspects of the self are constructed.90 Professor Timothy Macklem argues that "[t]he isolating shield of privacy enables people to develop and exchange ideas, or to foster and share activities, that the presence or even awareness of other people might stifle. For better and for worse, then, privacy is sponsor and guardian to the creative and the subversive.91 A meaningful measure of intellectual privacy should be erected to shield these activities from the normalizing gaze of surveillance. This shield should be justified on the basis of our cultural intuitions and empirical insights about the normalizing effects of surveillance. But it must also be tempered by the chilling-effect doctrine's normative commitment to err on the side of First Amendment values even if proof is imperfect.

Second, **mass surveillance uniquely disables social movements and activists to preserve elite dominance**

Lempert 2013, Law Professor Emeritus at Michigan

(Richard “PRISM and Boundless Informant: Is NSA Surveillance a Threat?” 6-13-13. http://www.brookings.edu/blogs/up-front/posts/2013/06/13-prism-boundless-informant-nsa-surveillance-lempert)

The 99.9% of us who pose no threat of terrorism and do not inadvertently consort with possible terrorists should not worry that the government will track our phone or internet exchanges or that our privacy will be otherwise infringed.

This does not mean, however, that the NSA programs and the capacities they reveal are of no concern. They should be regarded as canaries in the coal mine; they provide early warning of dangers we may be confronting. These capacities, along with increasingly ubiquitous surveillance cameras, photo recognition software, the ongoing development of rapid recognition DNA analysis, drones that can spy or kill and DNA, fingerprint, photo and other searchable digital databases together create what I have called the infrastructure of tyranny.

These technologies potentially enable small groups of people to control and restrict the freedom of far larger numbers. We think this could not happen here, and I do not claim it is imminent, but recent trends in politics and social life suggest that if the fear was ever groundless, it no longer is. Not only are our politics deeply and too often viciously divided, but divisions seem to be stoked by extremists who personally profit from their ability to arouse emotions and by small numbers of extremely wealthy individuals who spend freely to advance their views of the good society. Moreover, our political parties and Congress itself sometimes seem more interested in thwarting the opposition or scoring points with their most committed supporters than with cooperating and compromising to promote the national interest. Concerns raised by these developments are exacerbated by an increased tendency within Congress to ignore more or less neutral procedural commitments and understandings that have allowed effective governance despite sometimes deep differences in political goals. In addition, we live in a time of increasing inequality and decreasing social mobility. The experience of other countries from the French Revolution on suggests that when inequality becomes too great and a small group of “haves” is seen as capturing too large a share of the pie, protests begin that even if peaceful at the start are prone to erupt into violence. Even before violence from below erupts, and almost always afterwards, we have seen those on top muster their resources to suppress dissent and to preserve their positions of power, using violence of their own if need be. Historically the masses tend, sooner or later, to prevail, but in PRISM, Boundless Informant and other new technologies we are developing a set of tools that make it more likely that an elite core will be able to disrupt nascent revolt and maintain its preferred position by increased surveillance and even selective killing. Although it is not likely, it is not unimaginable that a future administration could, with substantial popular support, use a genuine crisis as an excuse to postpone a scheduled election, could put down subsequent protests with violence and could create a situation in which it maintained itself in power using the infrastructure we are creating to protect us from crime and terrorism. Even if the possibility is small it cannot be too much diminished. Doing this is likely to involve combating inequality, strengthening democratic institutions and perhaps abandoning the volunteer army, matters too far afield to be further discussed here. Even if it seems fanciful to fear that American democracy could one day be imperiled by technologies and activities developed to fight crime and terrorism, it is not farfetched to recognize the degree to which foreign governments can, and to some degree are, using these technologies to enable powerful elites to control people who desire more freedom or might seek to replace them in power. Moreover the lines demarcating those in control may relegate people of certain religions, gender, or gender preferences or ethnic heritage to permanent positions of economic disadvantage and powerlessness.

Third, warrantless mass surveillance is discriminatory

-Cannot analyze mass surveillance without seeing racism

Kumar & Kundnani 2015,

Assoc Prof Middle East Studies @ Rutgers and Research Fellow @ International Center for Counter Terrorism and NYU

[Deepa, Author of Islamophobia and the Politics of Empire (Haymarket Books, 2012); Arun , “Race, surveillance, and empire” – International Socialist Review - Issue #96 – Spring - http://isreview.org/issue/96/race-surveillance-and-empire]

Beginning in June 2013, a series of news articles based on whistle-blower Edward Snowden’s collection of documents from the National Security Agency (NSA) took the world by storm. Over the course of a year, the Snowden material provided a detailed account of the massive extent of NSA’s warrantless data collection. What became clear was that the NSA was involved in the mass collection of online material. Less apparent was how this data was actually used by the NSA and other national security agencies. Part of the answer came in July 2014 when Glenn Greenwald and Murtaza Hussain published an article that identified specific targets of NSA surveillance and showed how individuals were being placed under surveillance despite there being no reasonable suspicion of their involvement in criminal activity.1 All of those named as targets were prominent Muslim Americans. The following month, Jeremy Scahill and Ryan Devereaux published another story for The Intercept, which revealed that under the Obama administration the number of people on the National Counterterrorism Center’s no-fly list had increased tenfold to 47,000. Leaked classified documents showed that the NCC maintains a database of terrorism suspects worldwide—the Terrorist Identities Datamart Environment—which contained a million names by 2013, double the number four years earlier, and increasingly includes biometric data. This database includes 20,800 persons within the United States who are disproportionately concentrated in Dearborn, Michigan, with its significant Arab American population.2 By any objective standard, these were major news stories that ought to have attracted as much attention as the earlier revelations. Yet the stories barely registered in the corporate media landscape. The “tech community,” which had earlier expressed outrage at the NSA’s mass digital surveillance, seemed to be indifferent when details emerged of the targeted surveillance of Muslims. The explanation for this reaction is not hard to find. While many object to the US government collecting private data on “ordinary” people, Muslims tend to be seen as reasonable targets of suspicion. A July 2014 poll for the Arab American Institute found that 42 percent of Americans think it is justifiable for law enforcement agencies to profile Arab Americans or American Muslims.3 In what follows, we argue that the debate on national security surveillance that has emerged in the United States since the summer of 2013 is woefully inadequate, due to its failure to place questions of race and empire at the center of its analysis. It is racist ideas that form the basis for the ways national security surveillance is organized and deployed, racist fears that are whipped up to legitimize this surveillance to the American public, and the disproportionately targeted racialized groups that have been most effective in making sense of it and organizing opposition. This is as true today as it has been historically: race and state surveillance are intertwined in the history of US capitalism. Likewise, we argue that the history of national security surveillance in the United States is inseparable from the history of US colonialism and empire.

# Advantage 2: Exceptional access

Federal law enforcement officials are on a crusade to compel US companies and service provides to grant “exceptional access” or “golden key” access to all encryption developed in the US. This is a terrible idea.

First, Congress poised to pass cyber-sharing legislation immunizing companies

Mitchell July 20, 2015

[Charlie, “Senate, once again, looks to bring back CISA, Washington Examiner, July 20, 2015, <http://www.washingtonexaminer.com/senateonceagainlookstobringbackcisa/article/2568396>

In a major breakthrough, Senate leaders are pledging to bring up a long-stalled information-sharing legislation before decamping in three weeks for a month-long recess. Senate Majority Leader Mitch McConnell, RKy., said the bill would reach the floor this summer. Majority Whip John Cornyn, R-Texas, told The Hill newspaper last week that the bill will be considered sometime the week of Aug. 3, just before the Senate adjourns for its summer break on Aug. 7. "I think it will be on the floor this work period," a newly optimistic Senate Intelligence ranking member Dianne Feinstein, D-Calif., told InsideCybersecurity.com. Feinstein cosponsored the bill with Intelligence Chairman Richard Burr, RN. C., and has been championing info-sharing legislation over the past three Congresses. Action on this bill is the top priority for congressional leaders on cybersecurity issues, and for major trade associations representing the nation's critical infrastructure such as banks, telecommunications, gas and electricity, and many others. The House passed similar legislation in April, merging bills produced by the Intelligence and Homeland Security committees in that chamber. The legislation would allow companies to share with the government any threat indicators popping up on their networks that signal an unfolding cyberattack. It includes liability protection shielding the companies from certain lawsuits, and government regulatory actions related to the data they share. The business community and many in government — including the Obama administration — agree that at least some level of immunity is needed; otherwise companies simply won't take the legal risk of exchanging cyber information with government. The appropriate level of protection has been the sticking point going back to at least 2012. There is work to do — within the Senate, between the House and Senate, and between lawmakers and the White House. But info-sharing legislation now appears closer than ever to completion. If the Senate can pass its bill before the August recess, three-cornered House-Senate-White House negotiations can get started. The Senate and House versions contain different approaches to liability protection for industry, the government entities that can receive threat data directly from companies, and on a handful of other matters. The House also included a seven-year sunset in its legislation, meaning a future Congress would have to reauthorize the program-amendments on their own cybersecurity priorities during the CISA bill debate, which could further complicate final passage. Sen. Sheldon Whitehouse, DR. I., last week said he plans to offer an amendment creating a national databreach notification standard. He will also offer his proposal on updating criminal laws to fight hacking. The cyber infosharing bill seems to be advancing, which comes as a huge relief to its supporters. But this could get messy.

Second, Federal law enforcement is pushing hard for “golden key” access to open any encrypted communications

Shevinisky 2015 CEO Jekudo Privacy Company

[Elissa, “Opinion: Why the US government must lose cryptowars 2.0”, Passcode, July 23, 2015, http://www.csmonitor.com/World/Passcode/2015/0723/OpinionWhytheUSgovernmentmustlosecryptowars2.0

The battlefield landscape has changed since the '90s: Back then, encryption for commercial use was just starting to take off. These days, strong encryption powers our banking and ecommerce, and is increasingly implemented by major consumer tech companies. Apple said that devices running its new software would be encrypted by default. Even the company itself unable to gain access to its customers' protected data. And Google made headlines last year when it announced that "fulldisk encryption," which protects user information on its Android devices, would be enabled by default. The technology ecosystem may have changed over the last twenty years, but the ask from the national security establishment is, essentially, the same demand it made in the first cryptowars go round. Calling it “exceptional access” or a “golden key,” US officials want law enforcement offices to have special access to encrypted messages. They have relied on intercepting our communications as a way to find and prosecute criminal activity – missions they say strong encryption could thwart. The FBI and NSA want tech companies, such as Apple and Google, to design their encryption so that the government would have a set of keys to access the otherwise secure data. Insisting that groups such as ISIS, foreign state spies and criminals here at home are taking advantage of secure communications employing encryption, FBI Director James Comey wants a "secure golden key" for law enforcement to access the content of encrypted communications if officers get a courtordered warrant. NSA Director Adm. Michael Rogers has been more technically specific in his request, proposing a "split key” which would require the cooperation of multiple government agencies in order to use the key and decrypt the data.

Third, “exceptional access” massively heightens vulnerability

Washington Post Editorial July 22, 2015

http://www.nhregister.com/opinion/20150722/editorial-putting-the-digital-keys-to-unlock-data-out-of-reach-of-authorities

But there are legitimate and valid counter arguments from software engineers, privacy advocates and companies that make the smartphones and software. They say that any decision to give law enforcement a key — known as “exceptional access” — would endanger the integrity of all online encryption, and that would mean weakness everywhere in a digital universe that already is awash in cyberattacks, thefts and intrusions. They say that a compromise isn’t possible, since one crack in encryption — even if for a good actor, like the police — is still a crack that could be exploited by a bad actor. A recent report from the Massachusetts Institute of Technology warned that granting exceptional access would bring on “grave” security risks that outweigh the benefits.

The SSRA bans federal efforts to impose “exceptional access”

# **Advantage 3: The Free Internet NSA surveillance driving erosion in support for free internet**

First, US surveillance used to justify closing internet

Washington Post citing Freedom House in 2014

(Citing a Freedom House report. “In the ‘global struggle for Internet freedom,’ the Internet is losing, report finds” 12-4-14. http://www.washingtonpost.com/blogs/the-switch/wp/2014/12/04/in-the-global-struggle-for-internet-freedom-the-internet-is-losing-report-finds/)

The year 2014 marks the moment that the world turned its attention to writing laws to govern what happens on the Internet. And that has not been a great thing, according to an annual report from the U.S.-based pro-democracy think tank Freedom House. Traditionally, countries eager to crack down on their online critics largely resorted to blocking Web sites and filtering Internet content, with the occasional offline harassment of dissidents. But that has changed, in part because online activists have gotten better at figuring out ways around those restrictions; Freedom House points to Greatfire, a service that takes content blocked in mainland China and hosts it on big, global platforms, like Amazon's servers, that the Chinese government finds both politically and technologically difficult to block. In the wake of these tactics, repressive regimes have begun opting for a "technically uncensored Internet," Freedom House finds, but one that is increasingly controlled by national laws about what can and can't be done online. In 36 of the 65 countries surveyed around the world the state of Internet freedom declined in 2014, according to the report. Russia, for example, passed a law that allows the country's prosecutor general to block "extremist" Web sites without any judicial oversight. Kazakstan passed a similar law. Vietnam passed decrees cracking down on any critiques of the state on social media sites. Nigeria passed a law requiring that Internet cafes keep logs of the customers who come into their shops and use their computers. There's a bigger worry at work, too, Freedom House says: the potential for a "snowball effect." More and more countries, the thinking goes, will adopt these sorts of restrictive laws. And the more that such laws are put in place, the more they fall within the range of acceptable global norms. Also shifting those norms? According to Freedom House, "Some states are using the revelations of widespread surveillance by the U.S. National Security Agency (NSA) as an excuse to augment their own monitoring capabilities, frequently with little or no oversight, and often aimed at the political opposition and human rights activists."

**Second, surveillance damages US internet leadership**

Sinha of the ACLU and others in 2014

[Human Rights Watch, *With liberty to monitor all: How large-scale us surveillance is harming journalism, law and American democracy*]

The questions raised by surveillance are complex. The government has an obligation to protect national security, and in some cases, it is legitimate for government to restrict certain rights to that end. At the same time, international human rights and constitutional law set limits on the state’s authority to engage in activities like surveillance, which have the potential to undermine so many other rights. The current, large-scale, often indiscriminate US approach to surveillance carries enormous costs. It erodes global digital privacy and sets a terrible example for other countries like India, Pakistan, Ethiopia, and others that are in the process of expanding their surveillance capabilities. It also damages US credibility in advocating internationally for internet freedom, which the US has listed as an important foreign policy objective since at least 2010. As this report documents, US surveillance programs are also doing damage to some of the values the United States claims to hold most dear. These include freedoms of expression and association, press freedom, and the right to counsel, which are all protected by both international human rights law and the US Constitution.

Third, Free Internet is historically unique protection against societal collapse.

Dr. Eagleman 2010, Baylor College of Medicine

[David, Neuroscientist at Baylor College of Medicine, “ Six ways the internet will save civilization,” Wired, 9 Nov 2010, <http://www.wired.co.uk/magazine/archive/2010/12/start/apocalypse-no>]

Many great civilisations have fallen, leaving nothing but cracked ruins and scattered genetics. Usually this results from: natural disasters, resource depletion, economic meltdown, disease, poor information flow and corruption. But we’re luckier than our predecessors because we command a technology that no one else possessed: a rapid communication network that finds its highest expression in the internet. I propose that there are six ways in which the net has vastly reduced the threat of societal collapse. Epidemics can be deflected by telepresence One of our more dire prospects for collapse is an infectious-disease epidemic. Viral and bacterial epidemics precipitated the fall of the Golden Age of Athens, the Roman Empire and most of the empires of the Native Americans. The internet can be our key to survival because the ability to work telepresently can inhibit microbial transmission by reducing human-to-human contact. In the face of an otherwise devastating epidemic, businesses can keep supply chains running with the maximum number of employees working from home. This can reduce host density below the tipping point required for an epidemic. If we are well prepared when an epidemic arrives, we can fluidly shift into a self-quarantined society in which microbes fail due to host scarcity. Whatever the social ills of isolation, they are worse for the microbes than for us. The internet will predict natural disasters We are witnessing the downfall of slow central control in the media: news stories are increasingly becoming user-generated nets of up-to-the-minute information. During the recent California wildfires, locals went to the TV stations to learn whether their neighbourhoods were in danger. But the news stations appeared most concerned with the fate of celebrity mansions, so Californians changed their tack: they uploaded geotagged mobile-phone pictures, updated Facebook statuses and tweeted. The balance tipped: the internet carried news about the fire more quickly and accurately than any news station could. In this grass-roots, decentralised scheme, there were embedded reporters on every block, and the news shockwave kept ahead of the fire. This head start could provide the extra hours that save us. If the Pompeiians had had the internet in 79AD, they could have easily marched 10km to safety, well ahead of the pyroclastic flow from Mount Vesuvius. If the Indian Ocean had the Pacific’s networked tsunami-warning system, South-East Asia would look quite different today. Discoveries are retained and shared Historically, critical information has required constant rediscovery. Collections of learning -- from the library at Alexandria to the entire Minoan civilisation -- have fallen to the bonfires of invaders or the wrecking ball of natural disaster. Knowledge is hard won but easily lost. And information that survives often does not spread. Consider smallpox inoculation: this was under way in India, China and Africa centuries before it made its way to Europe. By the time the idea reached North America, native civilisations who needed it had already collapsed. The net solved the problem. New discoveries catch on immediately; information spreads widely. In this way, societies can optimally ratchet up, using the latest bricks of knowledge in their fortification against risk. Tyranny is mitigated Censorship of ideas was a familiar spectre in the last century, with state-approved news outlets ruling the press, airwaves and copying machines in the USSR, Romania, Cuba, China, Iraq and elsewhere. In many cases, such as Lysenko’s agricultural despotism in the USSR, it directly contributed to the collapse of the nation. Historically, a more successful strategy has been to confront free speech with free speech -- and the internet allows this in a natural way. It democratises the flow of information by offering access to the newspapers of the world, the photographers of every nation, the bloggers of every political stripe. Some posts are full of doctoring and dishonesty whereas others strive for independence and impartiality -- but all are available to us to sift through. Given the attempts by some governments to build firewalls, it’s clear that this benefit of the net requires constant vigilance. Human capital is vastly increased Crowdsourcing brings people together to solve problems. Yet far fewer than one per cent of the world’s population is involved. We need expand human capital. Most of the world not have access to the education afforded a small minority. For every Albert Einstein, Yo-Yo Ma or Barack Obama who has educational opportunities, uncountable others do not. This squandering of talent translates into reduced economic output and a smaller pool of problem solvers. The net opens the gates education to anyone with a computer. A motivated teen anywhere on the planet can walk through the world’s knowledge -- from the webs of Wikipedia to the curriculum of MIT’s OpenCourseWare. The new human capital will serve us well when we confront existential threats we’ve never imagined before. Energy expenditure is reduced Societal collapse can often be understood in terms of an energy budget: when energy spend outweighs energy return, collapse ensues. This has taken the form of deforestation or soil erosion; currently, the worry involves fossil-fuel depletion. The internet addresses the energy problem with a natural ease. Consider the massive energy savings inherent in the shift from paper to electrons -- as seen in the transition from the post to email. Ecommerce reduces the need to drive long distances to purchase products. Delivery trucks are more eco-friendly than individuals driving around, not least because of tight packaging and optimisation algorithms for driving routes. Of course, there are energy costs to the banks of computers that underpin the internet -- but these costs are less than the wood, coal and oil that would be expended for the same quantity of information flow. The tangle of events that triggers societal collapse can be complex, and there are several threats the net does not address. But vast, networked communication can be an antidote to several of the most deadly diseases threatening civilisation. The next time your coworker laments internet addiction, the banality of tweeting or the decline of face-to-face conversation, you may want to suggest that the net may just be the technology that saves us.